IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

MELINA BERNARDINO, individually and on behalf of other similarly situated persons, Plaintiff, v. BARNES & NOBLE BOOKSELLERS, INC., Defendant	Civil Action No. 17-cv-4570 **CLASS ACTION COMPLAINT** **Jury Demand**

INTRODUCTION

1. This is a consumer digital privacy class action seeking money damages, statutory money damages, injunctive relief and declaratory relief on behalf of Plaintiff Melina Bernardino ("Plaintiff" or "Ms. Bernardino") and other similarly situated customers of Defendant Barnes & Noble Booksellers, Inc. ("Defendant" or "B&N") who purchased DVDs or other video media ("Video Media") from Defendant's online store (the "B&N Website").

2. Like many online retailers, Defendant integrates social media plugins on its website and encourages customers to share favorite products on one of these social networks by use of the plugin. In the case of Defendant B&N, the social media partners are Facebook, Twitter, Pinterest and Google+.

3. Whether or not the plugins are affirmatively clicked by the customer, however, Defendant knowingly causes each customer's personal information, including information that identifies the purchased Video Media, to be disclosed to the social media partners. With respect to Defendant's disclosures to Facebook, Defendant also causes the identity of the customer to be disclosed if the customer is a Facebook subscriber.

4. The federal Video Privacy Protection Act ("VPPA") and its New York state counterpart (the Video Consumer Privacy Act or "NY VCPA") both prohibit the disclosure of personally-identifiable video purchase records to third parties without the express written consent of the customer in a separate stand-alone consent form. In violation of these statutes, Defendant does not obtain any consent, let alone the required express consent, prior to disclosing video purchase records to Facebook.

5. To the contrary, Defendant falsely assures its customers in its website privacy policy that it will respect their preferences concerning their personal information and omits social media sites in the list of recipients of personal information. Worse, prior to August 5, 2016, Defendant affirmatively assured customers in its Privacy Policy that it would never "provide any of your information to social networking sites without your express consent." This language was removed on August 5, 2016. Defendant therefore is in violation of New York's consumer protection law (General Business Law § 349) which forbids deceptive consumer-oriented business practices in New York.

6. Defendant violated these laws knowingly. Defendant agreed to abide by Facebook's "Platform Policy" if using a Facebook social media plugin. The Platform Policy requires partners to comply "with all applicable laws and regulations in the jurisdiction where your app is available." Specifically, Facebook requires partner websites to "comply with the Video Privacy Protection Act (VPPA) and obtain any opt-in consent necessary to share data on Facebook." The VPPA is one of only three laws mentioned by name in this section of Facebook's Platform Policy. Subject to the Platform Policy, Defendant voluntarily integrated the plugin and chose the type of information to be shared with Facebook as a result of integrating the plugin.

7. On February 3, 2017, Plaintiff visited Defendant's online store via her smart phone. She purchased a DVD of a movie.[1] She is a Facebook subscriber but did not click any social media button on Defendant's webpage during the purchase process. Without her knowledge or express written consent, Defendant caused the identity of this DVD, the purchase price, her identity and hundreds of other data points to be disclosed to Facebook.

8. Plaintiff therefore brings this class action on behalf of a nationwide class of Facebook subscribers who purchased DVDs or other video media from the B&N Website (the "Class"). Plaintiff brings the following causes of action:

a. Violation of the Federal Video Privacy Protection Act, 18 USC § 2710 ("VPPA");

b. Violation of the New York Video Consumer Privacy Act (the "NY VCPA") (New York GBL §§ 670-675);

c. Violation of New York General Business Law § 349; and

d. Declaratory Relief pursuant to 28 USC § 2201.

JURISDICTION AND VENUE

9. This Court has subject matter jurisdiction pursuant to 28 USC § 1331 (federal question) because this action arises in part under a federal statute.

10. This Court also has subject matter jurisdiction pursuant to 28 USC § 1332(d) (CAFA jurisdiction) because the amount in controversy exceeds $5,000,000, exclusive of interests and costs, and at least one member of the class is a citizen of a state different from the Defendant.

[1] To protect the privacy of the Plaintiff and her family, the name of the movie is not disclosed in this document. Plaintiff can provide further information to Defendant on a confidential basis and to the Court *in camera* or under seal if requested.

11. This Court has supplemental jurisdiction over the state law claims under 28 USC § 1367(a) because it is so related to the federal claim that it forms part of the same case or controversy.

12. This Court has personal jurisdiction over the Defendant because Defendant is headquartered in New York and the violations occurred in New York. Defendant created and controls the B&N Website in the State of New York.

13. Venue is appropriate in this District pursuant to 28 USC § 1391(b)(1) because Defendant is headquartered in this District.

PARTIES

14. Plaintiff Melina Bernardino ("Plaintiff" or "Ms. Bernardino") is an adult domiciled in Boca Raton, Florida, who used her smart phone to purchase a DVD from Defendant. She is a Facebook subscriber now and was a subscriber at the time of purchase.

15. Defendant Barnes & Noble Booksellers, Inc. ("Defendant" or "B&N") is a wholly-owned subsidiary of Barnes & Noble, Inc. ("B&N Parent") and branded as Barnes & Noble. B&N Parent operates primarily through Defendant and both entities are headquartered at 122 Fifth Avenue, New York, NY, 10011. Defendant is a retailer of books, digital media, games, gifts, magazines, music, toys, e-readers and educational products through its online store (barnesandnoble.com) and more than 600 physical stores in the United States.

RELEVANT NON-PARTY

16. Facebook, Inc. ("Facebook") is a publicly traded Delaware corporation headquartered at 1 Hacker Way, Menlo Park, California, 94025. Facebook is the world's largest social media platform and provided the Software Development Kit used by Defendant in

connection with its use of the Facebook plugin. Facebook is not named as a defendant in this action but is a relevant non-party for discovery purposes.

FACTUAL ALLEGATIONS

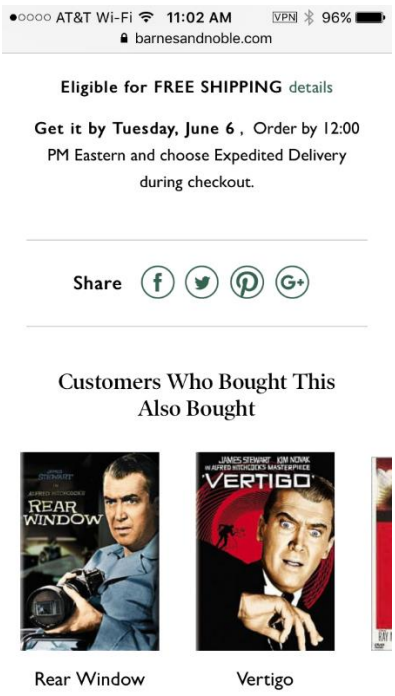
A. The Barnes & Noble Online Store Integrates Social Media Functionality

17. Defendant operates an online store accessible in the U.S. from a desktop at https://www.barnesandnoble.com, and from a mobile device at https://m.barnesandnoble.com.

18. When viewing a product description, the B&N Website displays four social media tools that allow customers to access their social media accounts and "post" (*i.e.*, "like" or otherwise share) their views of the product or the online store. For example, the product page of the DVD of the movie "The Man Who Knew Too Much" using a desktop computer (the Plaintiff purchased a different title) appears as follows:

19. As can be seen in the illustration above, the four social media tools ("plugins") are displayed immediately below the image of the product. Until last year, Defendant partnered with three social media platforms, and employed two separate Facebook plugins, instead of the one currently in use (as illustrated below):

20. If viewing the product description of the same DVD on a mobile device, the social plugins do not appear on the screen immediately below the product, but can be seen if the customer knows to scroll several pages down, as illustrated below:



21. The Defendant allows customers to complete a purchase in one of two ways. First, recurring customers can choose to sign into their accounts or new customers can choose to create an account. Alternatively, any customer can check out as a "guest" without signing into or creating an account. Because the store is an online store, however, even customers who check out as a guest must provide personal information for shipping and payment purposes.

22. During the checkout phase, Defendant does not display any visible social plugins. However, as noted below, Defendant does surreptitiously integrate *invisible* web beacons (also called "tracking pixels") that are relevant to the claims in this case.

B. Defendant Discloses Customer Information to Facebook

(1) How Social Plugins Work

23. Social media plugins are tools used by website developers and social media companies to facilitate the sharing of information by Internet users and, in many cases, between

websites and social media companies. The most ubiquitous plugins come from Facebook (including the "Like" and "Share" buttons) and other popular plugins are associated with Twitter, LinkedIn, Pinterest, Instagram (owned by Facebook), and Google+.

24. Social plugins serve two broad purposes:

a. First, social plugins allow users of partner websites to share their thoughts about a website, content or product with their social network, along with a link to the relevant website, content or product, by clicking on the plugin button.

b. Second (and less understood by the general public), plugins can be configured to allow the social networks to track internet users across the web -- whether or not the user ever clicks on the plugin, and whether or not the user is even a subscriber to the social network. This second feature of social plugins is not necessary to make the first feature functional.

25. When a website chooses to integrate a social plugin, it uses code (a Software Development Kit, or "SDK") that social media partners make available to first-party websites subject to various agreements not to misuse the SDK. Defendant used Facebook's SDK.

26. The initiating command from an Internet user to a website (the "GET request" or "GET command") instructs the website (here, the B&N Website) to return content requested for display on the user's browser. The B&N Website then responds by providing the requested data, thus allowing the browser to render the page on the user's screen.

27. Because the website integrates plugins, the website and its social media partner also instruct the browser to contact the social network for more data. This additional request asks for data to render the image of the plugin, but also transmits data regarding the user, the session with the first-party website, and the computer device.

28. In addition, the social network (here, Facebook) will send a query and a script specific to the B&N Website. For example, the query parameters related to a customer purchase of a DVD on the B&N Website include data regarding the purchased product, the price and the currency. Facebook will also set one or more Facebook user-identifying cookies and these cookies will be returned to Facebook with the product-identifying information.

(2) Referrer Headers

29. The data transmission from the browser to Facebook will include a detailed URL that contains some or all of the original GET request. These duplicate URLs are called "referrer headers" (usually misspelled "referer" due to a quirk of history).

30. Referrer headers are not just IP addresses. First-party websites have the option (but not the obligation) to include a variety of sensitive information, including search queries and file paths that are not necessary to share with social networks. Social plugins can function without detailed referrer headers being sent to the social network. Defendant, however, chooses to disclose the identity of the purchased product in the referrer headers.

31. Facebook publicly warned in 2012 about the privacy dangers possible with referrer headers. Facebook engineer Matt Jones wrote a blog post called "Protecting Privacy with Referrers" and noted:

> Here at Facebook, we're all about understanding how people interact with our site – including how they end up here from across the vast expanse of the internet. We're not the only ones, though – most web sites want similar insights about the people who use them.
>
> Despite its tragic misspelling, the HTTP standard's "referrer" header sent by browsers gives websites the information they need to see how users found them, and how they explore the sites once there.

Then under the heading "Referrers: not always welcome," Mr. Jones added:

> But sometimes referrers just don't belong – maybe there is sensitive information in a URL, or maybe a site just doesn't want its users' browsers telling others how they use the site. . . . Facebook is one site where referrers don't really belong . . .

(3) Cookies

32. In addition to a referrer header, the data transmitted to the social media partners may, by design, include one or more "cookies" residing on the user's browser. Cookies are small text files that web-servers can place on a person's web-browser and computing device when that person interacts with the web-server. Cookies can sometimes persist for years, and some can uniquely identify the user or the user's browser.

33. In the example of Facebook, one or more of the following cookies outlined in the chart below may reside on the user's browser and, if so, they are also packaged up and included with the referrer header:

Cookie	Sample Value	Information Contained	Expires
c_user[2]	10000004223456398	User's Facebook ID	Session / 1 mo.
datr	S3fJVgeTh7_ikK5frtHsHPmE	Browser ID	2 years
fr	0glRJJKaszKOLdKz8.AWXGH1RrxSLM3PHeHxfrORv10H8.BCVchV.Sj.FUJ.0.AWWsuv8a	Encrypted Facebook ID plus browser ID	1 month
lu	wfKm8ItfbXqRKlNoERo10H1H	Encrypted ID of the last user	2 Years
p	-2	User's channel partition	Session
presence	EM426705095EuserFA21B0911298286A2EstateFDutF1426705095426Et2F	Chat state	Session
s	Aa67DZudqH2wPH19	?	Session /1 mo.
xs	244%3AjIZKp45fK9ceMA%3A%3A1426705088%3A3455	Session number and secret	Session / 1 mo.
csm	2	Insecure indicator	Session / 1 mo.
act	1426704200575%2F14	Timestamp and counter of user actions	Session
wd	1280X653	Browser window dimensions	Session

[2] Facebook uses or has used several cookies to identify users, including the *a_user*, *c_user*, and *m_user* cookies.

(4) Device-Specific Information

34. Defendant also causes customers' device-specific information to be disclosed to Facebook in the transmissions caused by its integration of Facebook social plugins. According to Facebook's Data Policy, three types of data are caused to be transmitted:

a. Attributes, such as the OS, hardware, device settings, file and software names and types, battery and signal strength, and device identifiers.

b. Geolocation Information, including specific geographic locations, such as through GPS, Bluetooth or WiFi signals.

c. Connection Information, such as the name of the mobile operator or ISP, browser type, language and time zone, mobile phone number and IP address.

(5) Tracking Pixels

35. A Facebook tracking pixel, also known as a "tag" or "web beacon" among other names, is an invisible version of the social plugin that gets "rendered" with code from Facebook. It is frequently a single dot rendered either as a clear image (or the same color as the background), exactly one pixel in size. An example of the HTML snippet corresponding to the tracking pixel on the Defendant website would be: *https://www.facebook.com/tr?id =[redacted]&ev=PageView&noscript=1&v=2.0&if=false&dl=https://www.barnesandnoble.com/checkout/&rl=&_=[redacted]*, and it would appear quite literally as a single dot, as below:

36. The purpose of a tracking pixel (from Defendant's point of view) is to track conversion rates. If a retailer ran an advertisement for a DVD on Facebook, and 100 people clicked on the ad but only two purchased the DVD, the conversion rate is only two percent. By tracking precisely which customers responded to which ad and then actually committed to a sale, the retailer can tailor future ads better and increase the effectiveness of the ad.

37. The dark side of tracking pixels is the same as social plugins: by integrating a Facebook pixel, the retailer does not just call on Facebook to render the single dot on the browser – the retailer also causes the browser to disclose (in the request to render the pixel) exactly which of its subscribers are buying which DVDs, and also often causes the browser to disclose the same referrer headers, cookies and other personal information of the customer as if the pixel were a social plugin.

38. Worse, because tracking pixels do not have any role in social media sharing, they need not be visible to the person being tracked in order to function – and, by design, they are almost never visible. They also usually appear on the confirmation page (or close to it) at a later stage in the purchase session to ensure that only committed purchasers are being tracked. Thus, by using a Facebook tracking pixel, a retailer causes its customer's browser to disclose the same data to Facebook that would be disclosed with a social plugin, but does it even more surreptitiously, and after the product has either been placed in the customer's shopping cart or purchased.

39. The serious privacy problems raised by tracking pixels are well known. For example, until recently King County in Washington State used tracking pixels on its website, to track which users navigated to various government documents from various public service ads. However, because tracking pixels can never be anonymous, the county discontinued their use:

> **Privacy Concerns**
>
> Website tracking of this nature is a tactic employed by countless private-sector organizations, and probably some public-sector groups as well. But the data Facebook collects from its pixel feature is not anonymous and can be tied to individual users, often by name. If we allowed this, Facebook would know who did what on the King County website, and it most certainly would use that information to target advertisements to those people later on.

Derek Belt, *Why Facebook Pixels Are Not Allowed On Our Website* (Mar. 23, 2016).[3]

(6) Logged-Out and Logged-In Facebook Subscribers are Equally Affected

40. Defendant and Facebook cause the same video-identifying and user-identifying information to be disclosed regardless of whether the video purchaser is logged into his or her Facebook account at the time.

41. If a customer is logged into Facebook, the referrer header (containing video purchase data among other data points), one or more Facebook cookies, and the device identifiers are transmitted immediately. Facebook discloses on its Help Center page, for example, that simply by visiting a site with a Facebook social plugin, the customer's browser will be ordered to disclose "your user ID, the website you're visiting, the data and time and other browser-related info [sic]."

42. If a customer is not logged in, Facebook informs subscribers that it still receives information about the website being visited (i.e., the referrer header), date and time information and other browser-related information, but fewer cookies are included.

43. In addition (but not disclosed on the Help Center page), if the customer is not logged in at the time of purchase, the full referrer header and various parameter responses are set on the browser and transmitted later as soon as the customer logs back on, including user-

[3] https://www.govloop.com/community/blog/facebook-pixels-not-allowed-website/

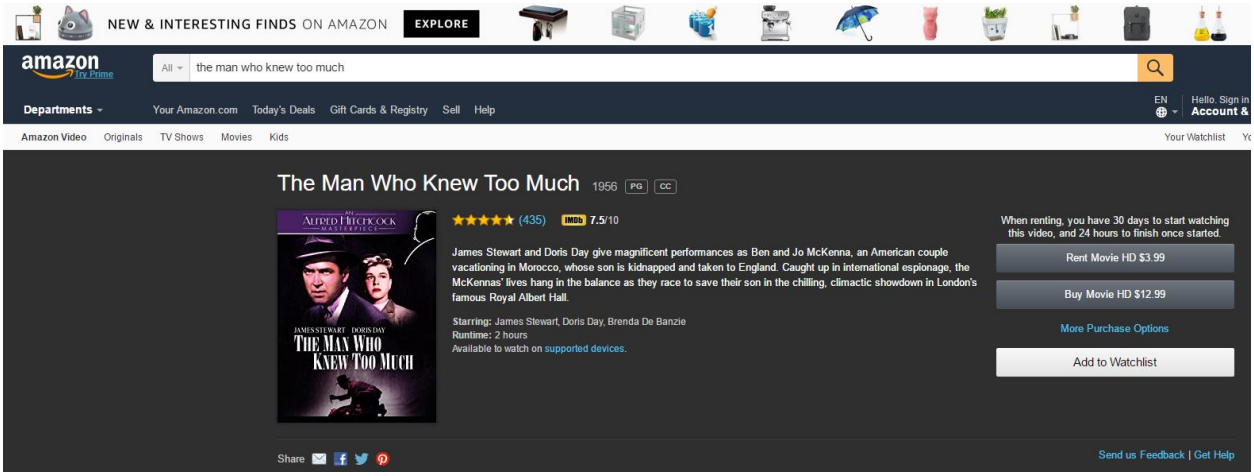
identifying cookies. Although the timing is different, Defendant still causes video-identifying and customer-identifying information to be transmitted to Facebook.

C. Disclosing Personal Information and Video-Identifying Information is Not Necessary

44. Social plugins and tracking pixels are not necessary for Defendant to conduct online commerce.

45. Even if a retailer found it useful to integrate Facebook social plugins and tracking pixels, Defendant is not required to disclose video-identifying and personal information to Facebook in the referrer headers and other code that it causes to be sent to Facebook. And as noted above, Facebook forbids the disclosure of such information without first complying specifically with the Video Privacy Protection Act and relevant state laws.

46. Other online retailers sell DVDs and integrate social plugins, but do not disclose video-identifying and personal information to Facebook. For example, like the B&N Website, Amazon.com sells DVDs and offers the ability to share thoughts about the product or website on social media by clicking on social buttons visible below the product, as show in the illustration below (the DVD in this illustration is not the DVD purchased by Plaintiff but shows the location of the plugins):



47. Although Amazon integrates social plugins in a location below the product precisely as Defendant does, unlike Defendant, Amazon does not disclose the identity of the video or any personally identifiable information to its social media partners, unless the customer chooses to click the plugin.

D. Facebook's Cookies, User IP Addresses and User Unique Device Identifiers are Personally-Identifiable to Facebook

48. Facebook earns revenue primarily through targeted advertising based on digital dossiers Facebook builds on each of its subscribers (and non-subscribers) from their activity on Facebook and elsewhere on the Internet.

49. Facebook's digital profiles are built in part through the use of cookies and other tracking technologies, such as pixels. In particular, of the Facebook cookies listed above in the chart in paragraph 33, Facebook tracks users with the following cookies:

a. The *c_user* cookie (like the *a_user* and *m_user* cookies) is the Facebook equivalent of a Social Security number. It is persistent and unique to each individual Facebook user.

b. The *datr* cookie is used by Facebook to individually identify each web-browser used to access Facebook. It is persistent and unique to each individual browser that access Facebook. If a computer is not a shared computer, then by definition a *c_user* cookie could be associated with a *datr* cookie. Even with a shared computer, there are a limited number of *c_user* cookies associated with any *datr* cookie. For example, in 2015, Facebook began allowing users to download portions of their Facebook data, including the last four digits of *datr* cookies Facebook associates with their user account, demonstrating that the *datr* cookies are associated with subscribers.

c. The *lu* ("last user") cookie is used by Facebook to individually identify the last Facebook user to log-in to Facebook using the browser at issue.

d. The *fr* cookie is an encrypted combination of the subscriber's unique Facebook ID and the browser ID. It essentially combines the *datr* and *c_user* cookies, and again demonstrates that *datr* cookies and *c_user* cookies are associated.

50. In addition to cookies, Facebook uses other data to personally identify users, stating that it "collect[s] information from or about the computers, phones, or other devices where you install or access our Services" and that it "may associate the information we collect from your different devices[.]" As noted above, among the information Facebook publicly acknowledges collecting to identify users includes: user device identifiers, IP addresses, phone numbers, specific geographic locations, and browser-fingerprint information.[4]

E. Plaintiff's Experiences

51. On February 3, 2017 Plaintiff visited Defendant's online store via her smart phone. She purchased directly from the B&N Website, not through Facebook. She was logged into her Facebook account at the time.

52. While on the B&N Website, Plaintiff searched for a DVD version of a specific movie. She did not click any social media button on the webpage at any time during the process.

53. During the purchase, she visited nine separate pages: (1) at the home page, she searched for the movie by name; (2) at the search results page, she selected the DVD; (3) at the product page, she added the chosen DVD to the cart and continued to checkout; (4) at the "Sign

[4] One report published by the Electronic Frontier Foundation estimated that, by using browser-fingerprinting alone, the likelihood that two separate users have the same browser-fingerprint is one in 286,777 or 0.00003487 percent. *See* Peter Eckersley, How Unique is Your Web Browser?, available at https://panopticlick.eff.org/static/browser-uniqueness.pdf. Browser-fingerprinting's accuracy is increased substantially where the tracking company also records a user's IP address and unique device identifier.

In" or "Check Out As Guest" page, she checked out as a guest; (5) she entered her shipping information; (6) she entered her delivery preferences (selecting express delivery); (7) she entered her payment information; (8) she reviewed her purchase; and (9) she viewed the submit and thank-you page. The entire process took approximately 2 minutes.

54. Without Plaintiff's knowledge or consent, in connection with this video purchase, Defendant caused the following data to be transmitted to Facebook:

a. the actual name and product number of the DVD;

b. the purchase price;

c. the currency designation (US dollars);

d. Plaintiff's IP address;

e. Plaintiff's Facebook *fr* cookie, which is an encrypted combination of her unique user ID and her browser ID; and

f. information regarding her mobile device, including but not limited to her phone number, geolocation, and her browser information.

55. Defendant never presented a consent form to the Plaintiff authorizing the disclosure of her purchase to any third party, and she was also never given the opportunity to opt out of Defendant's scheme to disclose the purchase to a third party.

F. Background of the VPPA and New York VCPA

56. The VPPA generally prohibits the knowing disclosure of a customer's video rental or sale records without the informed, written consent of the customer in a form "distinct and separate from any form setting forth other legal or financial obligations." Under the statute, the Court may award actual damages (but not less than liquidated damages of $2,500.00 per person), punitive damages, equitable relief and attorney's fees.

57. The VPPA was initially passed in 1988 for the explicit purpose of protecting the privacy of individuals' and their families' video rental, purchase and viewing data. As explained in the Senate report for the Act, "The impetus for this legislation occurred when a weekly newspaper in Washington published a profile of Robert H. Bork based on the titles of 146 films his family had rented from a video store." S. Rep. 100-599 at 6 (1988).

58. At the time of its passage, Congress was well aware of the impact of ever-changing computer technology. Upon the VPPA's introduction, the late Senator Paul Simon noted:

> There is no denying that the computer has revolutionized the world. Over the past 20 years we have seen remarkable changes in the way each of us goes about our lives. Our children learn through computers. We bank by machine. We watch movies in our living rooms. These technological innovations are exciting and as a nation we should be proud of the accomplishments we have made. Yet, as we continue to move ahead, we must protect time honored values that are so central to this society, particularly our right to privacy. *The advent of the computer means not only that we can be more efficient than ever before, but that we have the ability to be more intrusive than ever before*. Every day Americans are forced to provide to businesses and others personal information without having any control over where that information goes. These records are a window into our loves, likes, and dislikes.

S. Rep. No. 100-599 at 7-8 (1988) (emphasis added).

59. Senator Patrick Leahy also remarked at the time that new privacy protections were needed:

> It is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home … In an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. … I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.

S. Rep. No. 100-599 at 5-6 (1988).

60. Senator Leahy later explained:

> It really isn't anybody's business what books or what videos someone gets. It doesn't make any difference if somebody is up for confirmation as a Supreme Court Justice or they are running the local grocery store. It is not your business. It is not anybody else's business, whether they want to watch Disney or they want to watch something of an entirely different nature. It really is not our business.[5]

61. The sponsor of the Act, Rep. Al McCandless explained:

> There's a gut feeling that people ought to be able to read books and watch films without the whole world knowing. Books and films are the intellectual vitamins that fuel the growth of intellectual thought. The whole process of intellectual growth is one of privacy – of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye.

S. Rep. No. 100-599 at 7.

62. The legislative history of the VPPA shows Congress understood technology would soon make tracking "relatively easy" and the intent of the VPPA was to keep up with technology. "Unlike the other definitions in [the VPPA]," the definition of "personally-identifiable information" according the Senate Report, "uses the world 'includes' to establish a minimum, but not exclusive definition of personally-identifiable information." S. Rep. 100-599 at 12 (1988).

63. The New York VCPA was passed in 1993 (effective January 1, 1994) to supplement the VPPA. The two laws are similar, and the New York Legislature made the following legislative findings:

> The legislature finds and declares that the viewing of rented video tapes and movies in the home is a popular and widespread leisure pastime. Innumerable retail establishments in this state commonly record, often by computer, data containing the identities of consumers who have rented video tapes and movies and the titles of the videos rented. The large amounts of personally identifiable information collected by such

[5] GPO.gov, House Report 112-312, December 2, 2011, http:www.gpo.gov/fdsys/pkg/CRPT-112hrpt312/html/CRPT-112hrp312.htm.

> establishments, and the possibility of public dissemination of that information, pose a serious threat to the personal privacy of New Yorkers and is therefore a matter of state concern.
>
> It is the intent of the legislature by enactment of this article to protect the personal privacy of individuals and their families who rent video cassette tapes and movies and similar audio visual materials, without unreasonably restricting the ability of video tape service providers to collect and use information as is necessary to conducting their businesses.

New York GBL § 671 (declaration of legislative findings and intent).

64. Although similar, the federal statute and the New York statute differ in small ways, for example the New York statute distinguishes between a seller and renter of video media. But there is also one substantial difference: the New York statute requires the "informed written consent" to conform to a set form in at least ten-point bold faced font in clear view at the point of the transaction. New York GBL § 672(6).

G. Defendant Acted Knowingly

65. Defendant made the business decision to incorporate social media plugins from four different social media platforms. Defendant knew that, in the manner Defendant incorporated the plugins, even if a customer never clicks on a plugin, the SDK would cause personally identifiable information to be transmitted to the various social media platforms, including to Facebook.

66. Defendant agreed to comply with Facebook's Platform Policy as a condition of using the Facebook SDK and integrating a Facebook social plugin. Specifically, Defendant's "use of Facebook technology is subject to this Platform Policy, our Statement of Rights and Responsibilities and any other terms that apply to the applicable technology." Platform Policy § 6.19.

67. Facebook admits in its Platform Policy that Facebook will "receive information from you or in connection with your Platform integration in accordance with our Data Policy." Platform Policy § 6.3.

68. The information transmitted to Facebook from (and at the direction of) the partner website includes referrer headers and personally-identifying cookies. Indeed, Facebook cautions partners in its "Social Plugins" FAQs that when a person simply visits the partner website, even if the person does not click the social plugin button, Facebook will receive information about the webpage visited and the actual identity of the person:

> **What information does Facebook get when I implement a Social Plugin, and how is it used?**
>
> If a person has visited Facebook and visits your website with a social plugin, the browser sends us information in order to load Facebook content on that page. The data we receive may include info like the person's user ID, the website they're visiting, the date and time, and other browser-related info. We record some of this info and may use it to improve our products and services and to show people more interesting and useful ads.

69. While social plugin integration by definition will cause some data to be disclosed to Facebook, Defendant is not obligated to design the referrer headers to specifically identify the video being purchased. Defendant made that choice here.

70. Further, a website may utilize social sharing tools without disclosing personal information about its users to third-party social networks. For example, as described above, Amazon's website includes tools that customers can use to Share or Like products with others at the customer's discretion. But Amazon has chosen not to disclose personally-identifying information about its customers to Facebook. Defendant has made the opposite choice – to disclose personally identifiable information about its customers to Facebook.

71. Defendant also agreed, as a condition of using the Facebook SDK, that it would "[c]omply with all applicable laws and regulations in the jurisdiction where your app is available." Platform Policy § 5.8.

72. Defendant also agreed, "[i]f applicable, [to] comply with the Video Privacy Protection Act (VPPA) and obtain any opt-in consent necessary to share data on Facebook."

73. Prior to August 5, 2016, Defendant disclosed that its "Apps" (defined to include "content, software and mobile applications") may allow customers to provide information about purchases to social networks, but Defendant assured customers that it would never provide such information, at least not without express consent. Specifically, Defendant's Privacy Policy stated:

> **Interacting with social networking sites**
>
> Our Devices and Apps may provide you with the ability to enter (directly, or by authorizing us to download the information from a third party such as a social networking site or application) personal information such as contacts or lists of friends. These or related applications may also allow you to provide your information directly to social networking sites including information about your purchases, physical location, or comments. ***However, we will not provide any of your information to social networking sites without your express consent.***

Barnes & Noble Privacy Policy § 3 (emphasis added).

74. On August 5, 2016, the italicized language above was removed, indicating that Defendant knew that its social media integration was causing customer information to be disclosed to Facebook.

75. Finally, Defendant agreed that it would "[o]btain adequate consent from people before using any Facebook technology that allows us to collect and process data about them, including for example, our SDKs and browser pixels." Platform Policy § 2.11.

CLASS ACTION ALLEGATIONS

76. Plaintiff brings this class action pursuant to Federal Rule of Civil Procedure 23 on behalf of a national class (the "Class") defined as follows:

> All Facebook subscribers in the United States who purchased DVDs or other Video Media from the Barnes & Noble online store.

77. Excluded from the Class are Defendant and B&N Parent, their past or current officers, directors, affiliates, legal representatives, predecessors, successors, assigns and any entity in which any of them have a controlling interest, as well as all judicial officers assigned to this case as defined in 28 USC § 455(b) and their immediate families.

78. Numerosity: the Class Members are so numerous and dispersed nationwide that joinder of all members is impractical. Upon information and belief, the number likely is in the thousands. Class Members can be identified from Defendant's records and non-party Facebook's records.

79. Commonality: common questions of law and fact exist as to all Class Members and predominate over any questions affecting solely individual Class Members. These common questions include the following, among many others:

a. Whether Defendant integrated Facebook's SDK on its website;

b. Whether Defendant wrote the code knowingly or willfully;

c. What types of PII were disclosed due to the above acts;

d. The start and end dates of Defendant's practices;

e. Whether Defendant's actions violate federal law;

f. Whether Defendant's actions violate state law;

g. Whether Defendant's Privacy Policy is materially deceptive or misleading with respect to disclosures to social media partners;

h. Whether Defendant's actions occurred within the State of New York and within the United States of America;

i. Whether the Class Members are "consumers" within the meaning of the relevant federal and state statutes.

80. Typicality: Plaintiff's claims are typical of the claims of all other Class Members. Plaintiff purchased a DVD from Defendant's website and she is a Facebook subscriber. Defendant caused her PII and the identity of her Video Media purchase to be disclosed to Facebook without obtaining express written consent. Her claims are based on the same legal theories as the claims of other Class Members.

81. Adequacy: Plaintiff will fairly and adequately protect the interests of all Class Members in the prosecution of this action. Plaintiff is similarly situated with, and has similar injuries to, the Class Members she seeks to represent. Plaintiff is an adult and has retained counsel experienced in complex class action matters generally and in the emerging field of digital privacy litigation specifically.

82. Superiority: A class action is superior to all other available methods for the fair and efficient adjudication of this case, because joinder of all members is impractical if not impossible. Furthermore, the cost of litigating each claim individually might exceed actual and/or statutory damages available to each class member. There will be no difficulty in managing this action as a class action.

NON-APPLICABILITY OF ARBITRATION CLAUSE

83. Defendant's "Terms of Use" (also styled as the "Terms and Condition of Use") (the "TOU") contains an arbitration clause in the "Dispute Resolution" section purporting to

require arbitration of certain disputes – unless Defendant, at its sole discretion, elects to proceed in court.

84. Plaintiff, however, never agreed to the TOU, nor was she even aware of its existence. At no point during the purchase process was Plaintiff asked to agree to the TOU, nor even informed that a TOU existed. Defendant did not require Plaintiff to click a "check box" or otherwise affirmatively indicate assent to (or knowledge of) the TOU as a condition of purchasing the product when checking out as a "Guest."

85. Indeed, for any customer purchasing a DVD on a smart phone, the only mention of the TOU appears on the checkout page, only visible if the customer scrolls to the bottom of page. The website does not require the purchaser to scroll to the bottom of the page in order to check out.

86. Furthermore, Defendant's purported arbitration clause has terms that shock the conscience and no reasonable consumer (including Plaintiff) would ever knowingly agree to these terms. For example, in Section XVII of the TOU:

a. Defendant purports to retain to itself the sole right to disregard the arbitration clause and instead proceed in a "court of competent jurisdiction located in New York County, New York." This one-sided term is unfair on its face, but also could be used as a sword against out-of-state plaintiffs who cannot afford to proceed in court in New York.

b. Even worse, if Defendant elects to proceed in court, the TOU purports to waive customers' and Plaintiff's Constitutional right to a trial by jury.

c. If instead Defendant elects to arbitrate, it must be conducted by "telephone, online or based solely on written submissions" with no right of in-person appearances. This form of arbitration is notoriously anti-consumer.

d. Furthermore, the arbitration purportedly must follow the Commercial Arbitration Rules (including the Supplementary Procedures for Consumer-Related Disputes) which permit far less third-party discovery, if any. In this case, if third-party discovery from Facebook were required for Plaintiff to prove her claim, the purported agreement to arbitrate in effect shields Defendant from all liability.

ALLEGATIONS SUPPORTING INJUNCTIVE RELIEF

87. Plaintiff has been injured by Defendant's failure to comply with the VPPA and the New York VCPA.

88. Plaintiff will be irreparably harmed if an injunction does not issue enjoining the Defendant from continuing to evade its duty to obtain express written consent from customers prior to the sharing of video purchase data with third parties, including Facebook, Inc.

89. Plaintiff has no plain, speedy or adequate remedy at law.

90. Plaintiff is a Facebook subscriber and cannot stop Defendant from causing her personally identifiable video purchase records from being disclosed to Facebook. Even if she logs out of her Facebook account prior to making a purchase on Defendant's website, personally identifiable and video-identifying information about the Plaintiff is still disclosed at the time of purchase and again later when she logs back in.

COUNT I
Violation of the Video Privacy Protection Act ("VPPA")
18 USC § 2710

91. Plaintiff incorporates the above allegations by reference as if set forth fully herein.

92. The VPPA prohibits a "video tape service provider" from knowingly disclosing "personally-identifying information" concerning any consumer to a third-party without the "informed, written consent (including through an electronic means using the Internet) of the consumer." 18 U.S.C § 2710.

93. As defined in 18 U.S.C. §2710(a)(4), a "video tape service provider" is "any person, engaged in the business, in or affecting interstate commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audiovisual materials."

94. Defendant qualifies as a "video tape service provider."

95. As defined in 18 U.S.C. §2710(a)(3), "personally-identifiable information" is defined to include "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."

96. Defendant knowingly caused personally identifiable customer information and the product name, product ID, quantity, and purchase price of each and every Video Media purchased on its website to be disclosed to Facebook regardless of whether the consumer clicked on a Facebook social plugin. The personally identifiable information disclosed at the direction of Defendant to Facebook about purchasers of Video Media includes cookies, device identifiers, IP addresses, phone numbers, specific geographic locations, and browser-fingerprint information.

97. For Class Members logged into their Facebook accounts at the time of purchase, Defendant caused the purchase and personal information to be disclosed at the time of purchase. For Class Members not logged into their Facebook accounts at the time of purchase, Defendant caused the purchase and some personal information to be transmitted and additional personal information to be disclosed to Facebook at a later time when the customer next logs into Facebook

98. As defined in 18 U.S.C. §2710(a)(1), a "consumer" means "any renter, purchaser, or subscriber of goods or services from a video tape service provider." Plaintiff purchased a DVD from Defendant and thus is a consumer under this definition.

99. As set forth in 18 U.S.C. §27109(b)(2)(B), "informed, written consent" must be (1) in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer; and (2) at the election of the consumer, is either given at the time the disclosure is sought or given in advance for a set period of time not to exceed two years or until consent is withdrawn by the consumer, whichever is sooner." Defendant failed to obtain informed, written consent under this definition.

100. In addition, the VPPA creates an opt-out right for consumers in 18 U.S.C. § 2710(2)(B)(iii). It requires video tape service providers to also "provide[] an opportunity for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election." Defendant failed to provide an opportunity to opt out as required by the VPPA.

101. Defendant acted knowingly because it purposefully installed the SDK on its website that caused the data to be disclosed to Facebook and purposefully wrote the code that needlessly disclosed the actual identity of the purchased video materials and personally

identifiable information about its consumers to Facebook. Defendant also revised its Privacy Policy on August 5, 2016 to remove the representation that it would not disclose video purchase information to social media partners, indicating that Defendant was aware of its actions. Defendant also agreed to abide by the Facebook Platform Policy which requires website partners like Defendant to obtain consumer consent pursuant to any relevant law prior to sending data to Facebook.

102. As a result of the above violations, Defendant is liable to the Plaintiff and other Class Members for actual damages related to their loss of privacy in an amount to be determined at trial or alternatively for "liquidated damages not less than $2,500 per plaintiff." Under the statute, Defendant is also liable for reasonable attorney's fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendant in the future.

COUNT II
Violation of the New York Video Consumer Privacy Act ("NY VCPA")
New York General Business Law §§ 670-675

103. Plaintiff incorporates the above allegations by reference as if set forth fully herein.

104. Defendant created and controls the B&N Website in the State of New York.

105. The New York VCPA prohibits a "video tape seller" from "knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such seller" absent "informed written consent" of the consumer.

106. The term "consumer" is defined as "any renter, purchaser, or subscriber of goods or services from a video tape service provider or video tape seller." GBL § 672(1).

107. The term "personally identifiable information" is defined as "any information which identifies a person as having requested or obtained specific video materials or services from a … video tape seller." GBL § 672(3).

108. The term "video tape seller" is defined as "any person engaged in the business of selling prerecorded video cassette tapes or similar audio visual materials." GBL § 672(5).

109. The term "informed, written consent of the consumer" requires that a video tape seller, "prior to furnishing any video tape services shall offer the consumer an opportunity conforming to the notice [contained in the statute] to elect not to have personally identifiable information disclosed." GBL § 672(6).

110. Plaintiff and the Class are "consumers" under the New York VCPA because they are purchasers of goods and services from a video tape seller.

111. Defendant is a "video tape seller" because it is engaged in the business of selling prerecorded video cassette tapes "or similar audio visual materials." A DVD is audio visual material under the terms of the statute.

112. Defendant knowingly caused personally identifiable customer information and the product name, product ID, quantity, and purchase price of each and every Video Media purchased on its website to be disclosed to Facebook regardless of whether the consumer clicked on a Facebook social plugin. The personally identifiable information disclosed at the direction of Defendant to Facebook about purchasers of Video Media includes cookies, device identifiers, IP addresses, phone numbers, specific geographic locations, and browser-fingerprint information.

113. Defendant acted knowingly because it purposefully installed the SDK on its website that caused the data to be disclosed to Facebook and purposefully wrote the code that

needlessly disclosed the actual identity of the purchased video materials and personally identifiable information about its consumers to Facebook. Defendant also revised its Privacy Policy on August 5, 2016 to remove the representation that it would not disclose video purchase information to social media partners, indicating that Defendant was aware of its actions. Defendant also agreed to abide by the Facebook Platform Policy which requires website partners like Defendant to obtain consumer consent pursuant to any relevant law prior to sending data to Facebook.

114. Defendant failed to obtain consent from Plaintiff or any Class Member prior to disclosing the personally identifiable information in violation of GBL § 674.

115. Defendant is liable to the Plaintiff and other Class Members for "all actual damages [but] not less than five hundred dollars regardless of the amount of actual damage proved, plus costs, disbursements, and reasonable attorneys' fees." GBL § 675.

COUNT III
Violation of New York' Consumer Protection Statute
(General Business Law § 349)

116. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

117. Defendant created and controls the B&N Website in the State of New York.

118. New York General Business Law § 349(a) prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state."

119. Defendant engaged in material, deceptive, consumer-oriented acts in the conduct of its business in this state that injured Plaintiff and the Class.

120. In its privacy policy, Defendant falsely assures its customers that it will respect their preferences with respect to their personal information and omits social media sites in the list of recipients of personal information.

121. In addition, prior to August 5, 2016, Defendant affirmatively assured customers in its Privacy Policy that it would never "provide any of your information to social networking sites without your express consent."

122. In exchange for use of Facebook's SDK and tracking pixel code, Defendant agreed that it would "[o]btain adequate consent from people before using any Facebook technology that allows us to collect and process data about them, including for example, our SDKs and browser pixels." Platform Policy § 2.11.

123. Defendant further agreed that when using such technology, it would disclose the use of such technology and the sharing of customer information with "third parties." Specifically, Defendant agreed to inform customers:

> That third parties, including Facebook, may use cookies, web beacons, and other storage technologies to collect or receive information from your websites, apps and elsewhere on the internet and use that information to provide measurement services, target ads and as described in our Data Policy.

Platform Policy § 2.11(a).

124. Defendant failed to make the required disclosure above. Instead, in the portion of its privacy policy addressing "pixel tags or clear GIFs," Defendant only disclosed its possible use of tracking pixels in connection with marketing efforts. Defendant never disclosed that the pixels would be used to track customers who did not navigate to the site through ads or other marketing efforts, and Defendant also failed to mention which if any third parties would receive any personal information in connection with the pixels. Facebook is never mentioned:

> **Pixel tags or clear GIFs**
>
> We may use sensing technologies that use pixel tags or clear GIFs (which are also called web beacons). These technologies allow us to determine the effectiveness of our e-mail and advertising and marketing efforts. For this purpose, we tie the pixel tags and clear GIFs to personally identifiable information. We may also collect information regarding the links within such marketing materials that you click on and purchase statistics regarding item you buy following receipt of such marketing.

B&N Privacy Policy § 3(b).

125. Furthermore, Defendant never informs customers visually at the time of purchase that invisible tracking pixels are employed to collect purchase and personal data and send it to Facebook. When the product is first displayed, Defendant includes renderings of the various social plugins below the image of the product. Defendant's tracking pixels, however, are designed to be invisible and purchasers are not on notice of their use at the time of purchase.

126. As a direct and proximate result of Defendant's violation of § 349, Plaintiff and the Class have suffered actual damages in an amount to be determined at trial related to the loss of personal privacy which the Legislature found worthy of protection in GBL § 671.

127. Defendant willfully and/or knowingly violated § 349(a).

128. Section 349(h) provides a private right of action to enforce § 349(a) to recover each Plaintiffs' actual damages or $50 statutory damages per Class Member, whichever is greater.

129. Section 349(h) authorizes the Court to increase the amount not to exceed three times actual damages up to $1,000 per Class Member if the Court finds that Defendant willfully or knowingly violated this section.

130. Section 349(h) also authorizes the Court to award attorney's fees to a prevailing Plaintiff in addition to damages.

COUNT IV
Declaratory Relief
(28 USC § 2201)

131. Plaintiff incorporates the above allegations by reference as if set forth fully herein.

132. An actual and substantial controversy exists between Plaintiff and Defendant over the Defendant's duty to comply with the VPPA and New York VCPA.

133. This case is justiciable because the Defendant is currently in violation of federal and state law with respect to Plaintiff and all purchasers of video media.

134. Plaintiff's requested relief does not fall into any exception listed in 28 USC § 2201(a).

135. Declaratory relief will clarify the rights and obligations of the parties and any putative class members and is therefore appropriate to resolve this controversy.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court:

A. Certify this action as a Class Action pursuant to Rule 23 of the Federal Rules of Civil Procedure and appoints Plaintiffs as class representatives and their counsel as Class Counsel;

B. Award compensatory damages, including statutory damages, to Plaintiff and the Class for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;

C. Award restitution to Plaintiff and the Class against Defendant;

D. Award punitive damages in an amount that will deter Defendant and others from like conduct;

E. Permanently restrain Defendant and its officers, agents, employees and attorneys from violating the statutes referred to herein or otherwise violating its privacy policy and/or violating its customers privacy;

F. Award Plaintiff the reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

G. Grant Plaintiff such further relief as the Court deems appropriate.

JURY DEMAND

Plaintiff demands a trial by jury of all issues triable.

Dated: June 16, 2017
New York, NY

Respectfully submitted,

KAPLAN FOX & KILSHEIMER LLP

/s/ David Straite

Frederic S. Fox
David A. Straite
Joel B. Strauss
850 Third Avenue
New York, NY 10022
dstraite@kaplanfox.com
Tel.: 212.687.1980
Fax: 212.687.7714

BARNES & ASSOCIATES
Jay Barnes (*pro hac vice* to be sought)
219 East Dunklin Street, Suite A
Jefferson City, MO 65101
jaybarnes@zoho.com
Tel.: 573.634.8884
Fax: 573-635-6291

EICHEN CRUTCHLOW ZASLOW & McELROY
Barry R. Eichen (*pro hac vice* to be sought)
Evan J. Rosenberg (*pro hac vice* to be sought)
40 Ethel Road
Edison, NJ 08817
beichen@njadvocates.com
Tel.: 732.777.0100
Fax: 732.248.8273

KAPLAN FOX & KILSHEIMER LLP
Laurence D. King
Matthew George
350 Sansome Street
San Francisco, CA 94104
lking@kaplanfox.com
Tel.: 415.722.4700
Fax: 415.772.4707

WITES & KAPETAN P.A.
Marc Wites (*pro hac vice* to be sought)
4400 North Federal Highway
Lighthouse Point, FL 33064
mwites@wklawyers.com
Tel: 954.526.2729
Fax: 954.354.0205